X. The Benefits of Commercial Availability are also Achieved Through System Competition

Commercial availability of MVPD consumer equipment requires that consumers be able to purchase or lease equipment from non-network suppliers. Therefore, if consumers can obtain service from only a single MVPD service provider, for example, a local cable supplier, commercial availability requires that equipment be available through an outlet (retailer, manufacturer, etc.) that is not an affiliate of the service provider.

When consumers have access to multiple MVPD service providers, however, the benefits of commercial availability are obtained even if each service provider is the only source of consumer equipment that can be used on its system.[69] In this case, competition among MVPDs will lower equipment prices and spur innovation in the same way that having independent outlets does when there is a single MVPD. This is because an MVPD that faces competing service providers would risk not only the loss of equipment sales but also the loss of its subscribers if it were to raise the prices of its equipment. Here, competition among delivery systems provides the same benefits as does competition in the sale of equipment for any particular system.

For example, even if DBS service providers were the only suppliers of the dishes and converters that are necessary to receive their services, competition among providers ensures that equipment prices are competitive. As DBS service providers gain more popularity and penetration, their presence will increase the competitive constraints on the prices that other MVPDs can charge for both consumer equipment and their services.

[69] This is not to suggest that such MVPDs will find it in their interest to be the sole source of the equipment used on their systems.

At some point, therefore, the Commission may be able to conclude that there is sufficient competition among MVPDs to prevent any possible anticompetitive behavior in the supply of equipment. When this occurs, the commercial availability regulations can be abandoned because consumers can switch to alternative delivery systems if the price of equipment, and thus the price of receiving service, is increased. For example, when a cable system faces effective competition, sunset of the commercial availability rules is justified for that system.

XI. Private Industry Voluntary Standard-Setting is Preferable to Government Standards

Some degree of standardization may be needed to achieve the goal of permitting consumers to purchase set-top boxes at retail. For example, if the sale of separate security boxes is employed to achieve commercial availability, the interface between features boxes provided at retail and security boxes provided by the operator may have to be standardized to permit those consumers who wish to take advantage of the retail alternative to do so. A standardized interface permits features boxes obtained through retail outlets to be designed so that they can be connected to, and interact with, the separate security boxes obtained by subscribers from cable operators.[70] Nonetheless, this does not necessarily require that the interface standards be established by the government. Indeed, there are good reasons why this should not be the case.

[70] Standardization may also permit geographic portability of set-top boxes within a particular type of MVPD, or interoperability among different types of MVPDs. However, as we have argued above, defining such standards in detail risks inhibiting technological developments in consumer equipment by making it difficult or impossible to introduce new products that do not conform to the existing standard. It also increases the costs of this equipment.

A. Alternatives for Setting Standards

Broadly speaking, there are three ways to set standards. First, de facto standards may be established through the market. These standards result from the interaction of choices made by individual consumers and producers and not through any centralized process. Conformity to these standards is based entirely on self-interest since the only penalty for non-conformity is using a technology different from the one used by most others.[71]

Second, voluntary standards may be set through private industry standards organizations. These organizations, which typically operate by consensus among interested parties, establish standards through a process that involves information exchange and negotiation. The interested parties do most of the technical analysis themselves, but standards bodies occasionally engage in such analysis. The standards are voluntary in that even those who participate in determining them are not required to conform to them.

Standards organizations essentially serve three functions. First, they provide a forum in which individuals can express their views, so that the standards chosen take into account the perspectives of a wide range of interested parties. Second, they permit the parties to engage in "logrolling" in which a party may agree to accept a particular standard in return for agreement by others to support it at another time. Similarly, a single standard may incorporate design proposals from a number of different proponents in order to achieve consensus. Third, a standard established in this manner provides a "focal point" around which private actions can coalesce, thus reducing the probability that individuals will choose incompatible technologies.[72] Although it is

[71] Non-conformity would, of course, be a rational choice for those users who value the intrinsic characteristics of the non-standard product more than the benefits of being on a larger network.
[72] The importance of focal points in such situations is emphasized in T.C. Schelling, *The Strategy of Conflict*, Cambridge, MA: Harvard University Press, 1960.

possible to depart from the standard, there is a risk that others will not follow. For that reason, individuals who wish to be part of a dominant network will generally attempt to have the standard changed before departing from it. As in the case of de facto standards, conformity results from self-interest.

The third way in which to establish standards is though mandatory or de jure standards imposed by the government. Because these standards have the force of law, conformity by all parties is assured; as a result, individuals cannot deviate from them. Unlike the cases of de facto standards, which can be changed by market processes, or voluntary standards, where the standard effectively changes if enough individuals deviate from it, or if they agree to change it, mandatory standards can be changed only through a formal decision by a governmental body. As a result, mandatory standards are likely to be especially difficult to change.[73]

One important aspect of government standard setting should also be noted. David has pointed to the fact that "...governmental agencies are likely to have greatest power to influence the future trajectories of network technologies, just when a suitable informational basis on which to make socially optimal choices among alternatives is most lacking."[74] This phenomenon, which David refers to as the "blind giant" quandary, focuses on technologies that are changing rapidly where there is danger that a government decision that is difficult to reverse may be taken without adequate information.

---

[73] We are not claiming, of course, that de facto and voluntary standards are easy to change. Indeed, where network externalities are important, although conforming to these standards does not have the force of law, it is still difficult to change them. Our point is simply that the need for government action adds an additional difficulty to the process of changing a standard.

[74] P.A. David, op. cit., p. 210.

B. The Advantages of Private Standard Setting

In reaching a judgment about whether to use the de facto, private voluntary, or de jure processes, it is useful to distinguish between two (admittedly extreme) alternative types of standards. The first involves a situation in which there are a number of equally viable alternatives but it is important that everyone conforms to the same standard.[75] In this case, the problem is entirely one of coordination, so that having the government determine which of the alternatives is chosen may reduce the costs and uncertainty of having either de facto or voluntary standards. Private coordination may be difficult if there are a small number of adopters of each of the alternatives and each is reluctant to forego the benefits of having others switch to their standard. If either switching costs are small or the number of users who have to switch is small, and if the benefits of a common network are large, government action to break the logjam may produce significant benefits.[76]

At the other extreme is a situation where there are significant differences among the technologies competing to become the standard, and technological development is rapid. In this case, although there may be benefits from having *a* standard, *which* standard is ultimately chosen is likely to be at least as important. Moreover, because technology is changing, there may also be significant benefits from *delaying* the choice of a standard in order to obtain more information about the desirability of each of the alternatives. This poses some risk that a de facto standard may emerge, so that there may only be a limited period of time during which the government may affect the standard -- a problem that David characterizes as the "narrow window." However, where

[75] A good example would be the decision as to whether to have everyone drive on the left or right side of the road.

[76] Besen and Johnson, op. cit., p. 134, "By making a judgment in close cases, the government can help to prevent the excess inertia that might otherwise occur."

technology is changing rapidly, as in the MVPD navigation devices marketplace, there are likely to be more than offsetting benefits from the additional information that is obtained by waiting.[77] Indeed, the individual choices made by market participants in the absence of a standard may provide useful information to the government.

C. Private Industry Standard Setting is Already Occurring

The cable industry is currently engaged in a voluntary process to develop standards for digital subscriber equipment. This process has already resulted in widely-accepted standards for cable modems.[78] The Society of Cable Telecommunications Engineers (SCTE), a national standard setting body accredited by ANSI, has already issued specifications for digital transport and compression and system information[79] and detailed standards for emergency messaging and V-chip content are currently being considered. Consumer products manufacturers can use these published standards to build and market digital "cable ready" receivers that can receive and decode digital transmissions from cable systems and provide access to system information such as a channel guide. However, the receivers could not descramble secure information.

The Multimedia Cable Network System (MCNS) Partners Ltd., which represents most of the large MSOs, is establishing interfaces for digital cable system security elements. Specifications have been published for standard encryption methods and separate proprietary key management and delivery

[77] Id. p. 135, "The government should refrain from attempting to mandate or evaluate standards when the technologies themselves are subject to rapid change." This conclusion is based on the results of a number of case studies of standard setting in the broadcast industry.
[78] CableLabs has already released the MCNS Radio Frequency specification and eighteen vendors have agreed to comply with the specifications (*CableFax Daily*, Phillips Business Information, Inc., March 18, 1997, p. 1).
[79] These standards encompass many current international standards including MPEG-2 and Dolby sound.

systems. Encryption and decryption engines can be built and sold by any manufacturer, while the critical key delivery and management will be provided by a single manufacturer and its licensees.

These efforts have the advantage over government standard setting in that the parties involved have detailed knowledge of the various technical and cost issues that must be resolved in order to establish a workable interface, so that they can more easily take these issues into account. Because there are significant tradeoffs among standardization, variety, innovation, and costs, there is a real danger that, because the government is not as well informed, its participation in the process will do more harm than good.

XII. Compulsory Licensing is Neither Necessary Nor Desirable

In the Notice, the Commission asks whether it should "mandate that intellectual property rights be protected by a safeguard calling for licensing of such on reasonable and nondiscriminatory terms?"[80] and whether it can do so "without creating impediments to technological development or unnecessarily interfering with the competitive mechanisms involved."[81] This section addresses both of these issues.

We conclude that compulsory licensing of the technology employed in set-top boxes is neither necessary nor desirable. It is unnecessary because a good deal of voluntary licensing already exists as a result of a combination of demands by buyers for alternative equipment sources and the self-interest of manufacturers. Moreover, private, voluntary-standards organizations may also insist on licensing as a condition of incorporating particular technologies in the standards they adopt. Compulsory licensing is undesirable because, as the

[80] Notice, Para. 69.
[81] Id., Para. 70.

Commission correctly points out, it may "create impediments to technological development," which is especially important where, as here, the potential for rapid technical change is so great.

A. Voluntary Licensing is Occurring

There are well-known economic arguments that explain why the owner of a proprietary technology would wish to license the technology to one or more rivals at attractive rates.[82] The basic explanation for the existence of "second sourcing" is that it permits a firm to commit to low future prices or high future quality by putting a rival supplier in place to constrain its future behavior. The result is that the firm may increase the overall demand for the product because the commitment encourages buyers to "invest in the relationship."[83] Although the rival source now shares the market, the firm's profits can increase if the decline in its market share is more than offset by the growth in the size of the market.

Second sourcing can arise in two ways. First, a buyer may explicitly demand that a supplier put in place an alternative source as a condition of making a purchase. Alternatively, a seller may anticipate that its profits will increase if it commits to a second source and "voluntarily" contracts with an alternative supplier in order to provide assurances to potential buyers. In either case, the seller agrees to have a second source in order to expand the market

[82] See J. Farrell and N. Gallini, "Second-Sourcing as Commitment: Monopoly Incentives to Invite Competition," *Quarterly Journal of Economics*, 103, 673-694, 1988, and A. Shepard, "Licensing to Enhance Demand for New Technologies," *RAND Journal of Economics*, 18, 360-368, 1987.
[83] This phrase is due to J. Tirole, *The Theory of Industrial Organization*, Cambridge, MA: MIT Press, 1989, p. 34. Buyers may be unwilling to invest without a second source if they fear that they will be unable to prevent the seller from exploiting them after they have made the investment. This occurs when buyers must invest in assets that are specific to the seller and cannot effectively contract to prevent future exploitation.

and ultimately increase its profits.[84] The commitment can involve agreeing not to enforce intellectual property rights, ensuring the availability of information about technical advances in the product, and/or contracting for the price at which a key input will be supplied.[85]

Second sourcing is not merely a theoretical possibility. As Shepard observes:

> It is common practice in [the semiconductor] industry for an innovating firm – a firm that has developed and produces a new, proprietary product – to license one or more competing firms, thereby creating multiple sources of supply. Commentary in the trade press and by industry analysts attributes this practice to the innovating firm's desire to expand product demand. Second sourcing, it is claimed, makes the product more attractive to potential buyers.[86]

Moreover, the same practice occurs in the market for set-top boxes. For example, some cable operators require that manufacturers commit to a second source as a condition for making a major purchase.[87] In fact, General Instrument's contracts with MVPDs for the supply of digital boxes usually require the company to license other manufacturers. At present, General Instrument licenses its access control and other technology to a number of suppliers, including Pace Micro Technology, Hewlett-Packard, and Zenith Electronics. Licensees receive technical documentation and engineering support. Scientific-Atlanta licenses its PowerKey conditional access system to Pioneer.

---

[84] When Comcast announced it would buy 300,000 Scientific-Atlanta digital set-tops after first purchasing General Instrument digital set-tops, a Comcast source said that it was a matter of "second sourcing" in addition to concerns about General Instrument set-top availability (*Cable World*, March 24, 1997, p. 77).

[85] Note that it is in the interest of the seller that these commitments are, and are seen to be, binding because, otherwise, the higher profits sought by the seller may not materialize.

[86] A. Shepard, op. cit., pp. 360-361.

[87] It was recently reported that Time Warner Inc. expected to purchase one million digital set-top boxes with the initial 550,000 being provided by Scientific-Atlanta and the remaining boxes coming from S-A licensees Toshiba and Pioneer (*Wall Street Journal*, December 10, 1996, p. B10).

General Instrument also has licensing agreements with a number of manufacturers to produce and sell VideoCipher Integrated Receiver Descramblers (IRDs) for the C-Band consumer satellite receiving market. These licensees include Uniden, Toshiba, RL Drake, DX Communication, Echosphere Corporation, Tee Comm, Chaparral Communications, and Panasonic, although some of these are no longer engaged in production. Licensees are required to (a) meet certain financial requirements, (b) pay licensing fees, (c) meet certain design specifications, and (d) submit their products to GI for testing and approval.[88]

In addition to the licensing that comes about either through negotiations with buyers or unilateral actions by sellers, additional licensing may arise through the activities of private standards organizations. Indeed, it is common for standards organizations to require, as a condition of including a particular firm's technology in a standard, that the firm agree to license its technology to others at reasonable terms.[89] At that point, the firm can either agree to the requirement or attempt to market its product without the imprimatur of the standards body. It is reasonable to expect that such licensing terms will be the subject of on-going negotiations between the traditional MVPD equipment manufacturers and the manufacturers of consumer electronics equipment.

B. Compulsory Licensing is Likely to Impede Innovation

The Constitution and U.S. law recognize the need to provide adequate returns to innovators because the willingness of firms to invest in research and

[88] In addition to licensing second sources of consumer equipment, GI has licensed suppliers of the commercial IRDs used by cable operators. Licensees include Blonder Tounge Laboratories, DX Communications, Scientific-Atlanta, Pico Macom, Standard Communication, and Wegener Communications.

[89] For an example see T. Lefton, "IBM, Unisys Reduce Fees for Modem Compression," *Electronic News*, January 1, 1990, pp. 1, 34.

development depends on their ability to obtain returns that cover the risk-adjusted cost of their innovative activities. Although the returns to innovation are limited, through limitations on both the length and breadth of intellectual property protection, the returns would be reduced further if innovators were required to offer low-cost licenses to others. This would discourage some innovative activity that would otherwise occur. The question, therefore, is whether there are sufficient offsetting benefits from compulsory licensing of the technologies embodied in set-top boxes to compensate for the reduced level of research and development that such licensing would engender.

The previous analysis and the facts reported above both suggest that there is, and will continue to be, a considerable amount of licensing of GI and other manufacturers' technology without the need to resort to government-mandated compulsory licensing. That is, the choice is not between compulsory licensing and no licensing at all but between the amount of licensing that results from private action and the amount that would occur under government mandate.

Moreover, in the private dealings that give rise to the licensing, GI, like other manufacturers, is able to make the trade-off between the immediate demands of its customers and the long-term returns to its investments in research and development. That is, GI may be able to resist demands that it offer low-cost licenses by pointing out that higher prices are needed to support its research and development activities.

In contrast, a government agency is more likely to emphasize the effect of its policies on current prices and to minimize the effects that its policies have on innovation in the long run. As a result, the Commission is correct to be concerned about the "impediments to technological development" that a mandatory licensing requirement might create.

XIII. Summary and Conclusions

The existence of set-top boxes permits television viewers to obtain new services without having to replace their existing receivers. As these services become widely used, the capability to receive them tends to migrate to receivers so those consumers with new receivers can obtain these services without using auxiliary devices. Nonetheless, there is likely to be a continuing need for such devices because new services are continually being introduced, some services are insufficiently popular for the ability to obtain them to be profitably included in receivers, and MVPDs must maintain control over access to their services.

One way to ensure the commercial availability of set-top boxes may be through industry development of a standard interface that separates security from non-security components. Under this approach, MVPDs would offer separate boxes that provide security (and other network management functions) and provide information that permits independent manufacturers to design features boxes that can connect to, and interact with, the security-only boxes. If this approach is adopted, there is no reason for the Commission to prevent MVPDs from also offering boxes that integrate security and other functions.

Alternatively, commercial availability may be achieved through the provision at retail of boxes that integrate security and non-security functions. Given the potentially greater security risks and loss of efficiencies inherent in a separation model, the Commission should refrain from mandating separation as the sole way to effect commercial availability. More generally, the choice of which security method should be used to protect network signals and to ensure commercial availability should be left to the MVPD.

Although geographic portability and system interoperability of equipment may provide some benefits to consumers, these benefits are likely to be outweighed by the resulting costs. These include the higher costs of producing

equipment, the costs of the transition from the current system in which there is only limited portability, and the loss of variety, innovation, and experimentation that would necessarily accompany the standardization of equipment to achieve portability. Where portability and/or interoperability benefits consumers and are economically feasible, the marketplace has shown it will drive such results (the cable modem provides such an example). Thus, government mandates in this area are unnecessary and unwise.

The introduction of new types of equipment may require that they be offered at low, possibly below-cost, prices in order to assuage the fears of early adopters that they may be stranded on very small networks. Below-cost pricing of equipment may also legitimately be used to promote the sale of the MVPD's complementary services

Competition among systems constrains consumer equipment prices in the same manner as does competition among suppliers of equipment for the same system. As a result, the Commission can eliminate its commercial availability regulations when it concludes that a given MVPD faces effective system competition.

Because of the complexities of the technologies involved and the rapid rate of technical innovation in the MVPD marketplace, standards should continue to be established through private negotiations. For much the same reasons, the government's role in setting equipment standards should be limited.

Finally, the government should not impose mandatory licensing of the intellectual property of equipment manufacturers. Mandatory licensing would discourage technological innovation and is unnecessary in light of the substantial voluntary licensing that is already taking place.

APPENDIX B

Primer on Security Methods and Physical Implementation of Security

This Appendix provides an overview of analog and digital security methods in use and planned for broadband cable systems. It covers security for both video distribution and Internet access services. It also discusses the various physical implementations for securing digital video signals used by multichannel video programming distributors ("MVPDs") and the security implications of each.

1.0 Overview of Analog Video Security

A variety of analog video security methods have been employed over the years. The most commonly used today is addressable scrambling, whereby premium programming is transmitted in scrambled form from the cable headend, and the programming is descrambled in consumer terminals at the subscriber's premises. The descrambling is controlled by entitlement messages sent to each consumer terminal. Other analog security systems include non-addressable scrambling, interdiction, and traps.

1.1 Control Signaling and Key Management

Control signaling consists in part of messages addressed to consumer terminals which tell the controller in the terminal which scrambled programs to descramble. Each consumer terminal has a unique address or serial number, and entitlement messages are addressed to specific terminals. These messages are transmitted periodically and can be used to reprogram the terminal to descramble different programming services from one minute to the next in order to provide pay-per-view services.

Control signaling may be carried in the vertical blanking interval ("VBI") of an analog channel, in a separate out-of-band data channel, or in a combination of the two. The out-of-band data channel receives authorization messages and schedule information for pay-per-view programming. The consumer terminal contains a separate data channel receiver that is always tuned to the data channel, no matter what video channel is tuned. Data in the VBI of a scrambled channel contains information needed to descramble the program, such as when to invert the video, as well as channel identification and billing data.

In some system designs, there is no out-of-band data channel. In that case, all control signaling is carried in the VBI, and either the consumer terminal must be tuned to the specific video channel containing the signaling, or identical control information must be carried in the VBI of every video channel. This would require VBI encoders for many or all of the channels at the cable head end, broadcast as well as scrambled channels, thereby increasing system costs. In some of these systems, only the VBIs of scrambled channels carry the control information, which requires the consumer terminal to be tuned to a scrambled channel when the TV is turned off.

Out-of-band data is viewed as a more secure path for control signaling. This is because the channel may employ digital encryption, as well as proprietary modulation methods and protocols making it more difficult to intercept messages.

Upstream transmitters, related bandwidth management functions, and certain types of on-screen displays may also be considered part of cable system security control for pay-per-view programming services. The transmitters may operate on frequencies within the cable, or may use telephone lines. The upstream channel in a cable system is shared among multiple subscribers. The consumer terminal supplied by the cable operator assigns frequencies and adjusts transmitter power levels to prevent interference. Interference and perhaps loss of privacy would result if access to the upstream channel were not controlled by the cable operator. The menus and displays may be used for the selection of pay-per-view programming. These menus, and the upstream transmission of the subscriber's response to them, are essential to the cable system's accounting, billing, and recordkeeping for premium programming.

1.2 Analog Video Scrambling

A number of different technical methods are used to scramble analog TV signals in cable systems. The most common of these is "synch suppression" or "synch depression," a family of methods that includes suppressing the horizontal and/or vertical synch pulses by attenuating the RF envelope or shifting the baseband level prior to modulation. Synch restoration information may be sent instead on the sound carrier or in the VBI. The offset time for sending the synch information may be varied randomly from one video field to the next, to add complexity and security.

Other analog scrambling methods include video inversion or video/synch inversion (subtracting a constant RF carrier at the same frequency and phase as the actual RF carrier); frequency inversion; video jitter (start time of each scan line is randomly varied); time reversal (some lines are transmitted in time-reversed manner); line dicing (each scan line is split into two fragments at a random point, and these fragments are interchanged prior to transmission); and permutation of video lines. Most systems today use time-varying combinations of two or more of these analog scrambling methods.

Addressable analog consumer terminals contain the circuitry to descramble signals that are scrambled using the above scrambling methods, and, as noted, operate under the control of authorization or entitlement messages sent from the cable head end. But these analog methods, in contrast to digital encryption, are susceptible to signal processing circuits found today in pirate cable boxes that ignore the authorization messages, restore the suppressed synch pulse, and detect and correct for inversion and other techniques.

1.3 Other Analog Security Systems

Other analog security methods involve non-addressable scrambling, interdiction, and traps.

1.3.1 Non-Addressable Scrambling

With non-addressable scrambling, premium programming is scrambled at the head end and descrambled in consumer terminals at the subscriber's premises. These consumer terminals are pre-programmed so that they may descramble only certain previously-defined channels. If a subscriber changes the premium channels to which he/she subscribes, a technician must visit the subscriber premises to replace or modify the consumer terminal.

1.3.2 Interdiction

Two interdiction methods are available at this time. Under the first, premium programming is sent in the clear from the head end. At the subscriber's site, jamming oscillators are activated to block those channels to which the customer does not subscribe. With this approach, every subscriber premises must have an attached interdiction box. For the oscillators to be effective, they must be gain controlled to match the signal strength of the cable system signals, and filtering must be good since thousands of oscillators are active on the same frequencies at the same time.

With the second type of interdiction, premium programming is scrambled at the head end and is descrambled in a unit that is physically outside of the subscriber's premises. The descrambling unit may be addressable and thereby controllable from the cable head end. The most common design employs a single channel descrambler, which descrambles only on channel at a time. An alternative approach, under development by one company, would descramble all scrambled channels. Interdiction has not been popular because the descrambling unit is exposed to the elements, and because security is weakened when all of the channels are available "in the clear" outside a building.

1.3.3 Traps

There are two types of traps, positive and negative traps. With negative traps, the signal is sent down the cable in the clear, and a negative trap is installed outside a customer's premises to electrically degrade the quality of a single 6 MHz channel slot so that it may not be viewed. A separate circuit must be installed for each channel or block of adjacent channels that is being degraded. This approach has a number of disadvantages. First, while negative trap circuits are sometimes installed in a secured box outside the subscriber's premises, subscribers may force open the boxes and remove the trap circuits to steal the signals. Second, negative traps deteriorate over time and may become ineffective in blocking the programming from viewing. Finally, if many non-adjacent channels are to be controlled, then many trap circuits must be installed, which creates the risk of degrading other channels as well. However, in a small cable system with few premium programming services, trapping may be the most economical security method.

With positive trapping, a jamming carrier is inserted into the channel to be secured at the headend. The jamming signal is then filtered out at the subscriber's home with a trap circuit, very narrow in frequency, which removes the interfering carrier to allow viewing of the signal. This method is insecure because the trap is easy to build, even for the thief. Moreover, only a single trap is needed for the channel 3 or 4 output of a converter, rather than separate traps for each jammed channel.

The determination of whether to use negative or positive traps for a particular programming service is principally driven by the penetration of the service. For highly-penetrated services with stable subscriber bases, negative traps are used since fewer traps must be installed. For this same reason, positive traps are typically used for low-penetration services with established subscriber bases.

With both interdiction and trapping, there may be no need for navigation devices, and thus none to be made available for retail sale.

2.0 Overview of Digital Television Security

Digital television security differs from analog security in that analog security modifies the properties of the video signal to make it difficult or impossible to display on a standard TV receiver, while digital security applies general-purpose encryption methods to the digital bit stream that contains the video and audio signals. As with analog security, the digital decryption is controlled by entitlement messages sent to each consumer terminal, which generate decryption keys. While attacks on analog security typically employ circuitry to modify the properties of the video signal, attacks on digital security often focus on the entitlement messages, generation of keys, and identity, or address of the consumer terminal.

2.1 Cable Industry Digital Standards Efforts

The U.S. cable industry has agreed upon major elements of a digital cable system specification for North America. This specification incorporates MPEG-2 video and transport, Dolby AC-3 audio, and ITU-T Recommendation J.83 Annex B modulation (64 QAM and 256 QAM) and error coding. The standards work in this area is being done by the Society of Cable Telecommunications Engineers (SCTE).

The specification also incorporates the DES encryption standard as the core encryption system for digital video. Multiple conditional access systems, such as DigiCipher® II and PowerKEY® can be supported using this core encryption.

2.2 Digital NRSS

The security trend in the digital multichannel video industry, as well as the difference between renewable security and separation of security is best understood within the context of the National Renewable Security Standard ("NRSS") effort of the EIA/NCTA Joint Engineering Committee.

That group has developed a two-part security interface draft standard (IS-679) for multichannel digital video. The draft standard is now in the ballot process leading to adoption as an EIA standard and perhaps eventually as an ANSI standard.

NRSS provides two physical designs, one in part A and one in part B. Part A defines a removable and renewable security element physical design that is an extension of the ISO-7816 smart card standard. Part B defines a removable and renewable security element based on the PCMCIA ("PC Card") physical design. These designs are intended to allow either an NRSS-A or NRSS-B device to provide security for applications involving multichannel video programming services.

The main differences between NRSS-A and NRSS-B devices are the range of capabilities and the capacity for extension. The NRSS-A interface is limited to 8 electrical contacts using serial communication, whereas the NRSS-B interface uses 68 electrical contacts and parallel communication. Potentially, the NRSS-A device could be smaller and less costly, while the NRSS-B device could be more robust and extensible. The ISO smart card physical limitations in NRSS-A, coupled with the reported piracy experience in satellite video systems using ISO smart cards both in the U.S. and in Europe, suggest that an ISO smart card approach is not sufficiently secure nor sufficiently extensible to handle cable system security needs.

In applying the standard, an MVPD might choose to employ either the smart card or the PCMCIA card. A consumer electronics product that was sold commercially and intended to work with all MVPDs might have to support both types of cards, while a consumer terminal intended only for a single cable system or a single satellite system would need to support only the one used in that system. Since the NRSS will, when adopted, be a voluntary standard, any MVPD might choose some other renewable security interface instead. One popular approach is to begin with embedded security (i.e., the initial security chip is inside the consumer product), with an interface slot capable of accepting a future security card, if security needs to be upgraded (see section 4.3 below discussing hybrid security).

3.0 Cable Modem/Internet Access Security

Cable modem specifications are in the process of being standardized by the SCTE. Virtually the same modulation and transport used for digital MPEG video will be employed on cable modems, resulting in cost savings because of production volumes and component commonality.

Some of the specifications are being developed by Multimedia Cable Network System ("MCNS"), a coalition of cable TV operators. The final standard may include one or more specifications for security between the cable modem and the server located at the cable headend.

There is a debate within the cable industry on the level of security needed for this link. For Internet access and for most data networks, end-to-end security during a session is viewed as more appropriate than security on individual links. This is typically provided by software such as a secure browser.

Nonetheless, security on the modem-to-headend link may also be needed since that link is an RF channel that is shared by cable TV subscribers within a neighborhood. Thus, there may be a need to protect privacy by encrypting those transmissions on this link that would not otherwise be secured. A DES-based encryption method, similar or equivalent to the video encryption discussed above, would appear to be the best choice for security on this link. Additional techniques may be required for tiered access to value-added subscription data services.

4.0 Various Physical Implementations for Securing Digital Video

MVPDs are utilizing a variety of physical implementations for securing digital video. These implementations may be separated into the following four categories: 1) embedded; 2) totally removable and replaceable; 3) hybrid; and 4) split.

4.1 Embedded Security

Embedded security involves circuitry that is permanently installed within a cable converter or DBS receiver in an integrated unit. Nearly all addressable analog consumer terminals today use embedded security.

4.2 Removable Security

Removable security involves circuitry that may be totally extracted from the host device. This must at least involve a connector, which may or may not be accessible to customers. In other words, replacement of security may require opening the consumer terminal, which may not be feasible for most consumer terminals, since many have tamper-prevention switches and non-standard security fasteners. This is a more expensive approach than embedded security, because of the cost of the connector, cost of the card or board that carries the security circuitry, and possible need for duplication of components or functions both on the card and in the consumer terminal.

Moreover, removable security that is accessible to customers is potentially weaker security than embedded security. This is because it provides a convenient comparison of the encrypted data in with the decrypted data out, as well as access to a variety of signals including entitlement messages and other control data that appear at the connector. In contrast, comparable signals are buried deeply within the circuitry in an embedded security design.

4.3 Hybrid Security

A hybrid security system uses embedded circuitry but, if necessary, this circuitry may be upgraded or overridden with new elements. Thus, embedded security may nonetheless be replaceable. This approach has the benefit of a lower initial cost than a totally-replaceable approach, because the consumer terminal is initially supplied without the replacement card. But because it supports renewal of security if security is broken, it retains the full security of a removable design. This is the security design approach that is currently used by Primestar consumer terminals and

which will most likely be employed in most digital cable systems in the United States. Most current digital consumer terminals being supplied today use this approach, although the replacement of the security element in today's terminals may have to be done by a technician rather than the subscriber if the connector for the plug-in replaceable element is enclosed within the consumer terminal.

4.4 Split Security

A split security system has both embedded circuitry that supports some security functions (e.g., descrambling) and replaceable circuitry that supports other security functions (e.g., key management). This approach allows the high-speed signal processing (decryption of the high-speed video) to be done within the consumer terminal, while the low-speed processing of keys and entitlement messages is done on the card. It is therefore likely to be less expensive than removable security. This is the design approach used by the DirecTV system. However, it has the disadvantage that the control signals appear on the connector, a weakness that has been successfully exploited by pirate card suppliers.

The NRSS standard, discussed above, could be employed in connection with any of these approaches that employ some element of replaceability, e.g., removable, hybrid, or split security. However, the NRSS standard does not by itself support out-of-band data channels, as is used by cable systems to carry control signals and entitlement messages addressed to specific subscribers.

General Instrument believes that a hybrid security approach for digital cable devices, because it provides for replacement of security in case the security is compromised, may be designed to be sufficiently secure to be sold at retail. However, testing of specific designs in the marketplace may be necessary before the industry is sufficiently confident of this.

APPENDIX C

DIGICIPHER® II/MPEG-2:

OPEN STANDARDS, LICENSING, AND COMPLETE SYSTEM DEVELOPMENT

Marc L. Tayer

General Instrument Corporation

April 1997

1. Introduction

Now that the International Standards Organization (ISO) MPEG-2 standards for video coding and transport/multiplexing are finalized, virtually all digital television systems brought to market are MPEG-2 compliant. Other digital television standards, such as those adopted by the European Digital Video Broadcasting (DVB) group, the United States Advanced Television Systems Committee (ATSC), the International Telecommunications Union (ITU), and the Society of Cable Telecommunications Engineers (SCTE), are becoming equally important.

With multiple standards bodies working on various aspects of digital communications systems, General Instrument's philosophy in developing its DigiCipher® II/MPEG-2 and Magnitude DVB digital television systems is to select open standards whenever possible. The one exception is in the critical area of access control, which GI believes should remain proprietary in order to maximize system security.

General Instrument's DigiCipher II/MPEG-2 digital television system has been adopted by numerous programmers and network operators throughout the world. It is fundamentally a "system of standards" based on ATSC and SCTE, comprising:

- MPEG-2 Video
  (ATSC A/53 Annex A, SCTE DVS 033)
- Dolby® Digital AC-3 Audio
  (ATSC A/53 Annex B, SCTE DVS 018 Annex B)
- MPEG-2 Transport
  (ATSC A/53 Annex C)
- System Information (SI)
  (ATSC A/56, SCTE DVS 022 and 011)
- Subtitling
  (SCTE DVS 026)
- Trellis Coded 64/256 QAM Modulation and Forward Error Correction
  (ITU-T J.83B, SCTE DVS 031)
- QPSK Modulation and Forward Error Correction
  (ITU-R Draft Recommendation [11/38] System C)
- Data Encryption Standard (DES) Cipher Block Chaining
- DigiCipher II access control

General Instrument's Magnitude DVB system is also a "system of standards" based on DVB, including:

- MPEG-2 Video
- MPEG-2 Transport
- Musicam Audio
- DVB Cable and Satellite Modulation/Forward Error Correction
- DVB Service Information (SI)
- DVB Common Scrambling Algorithm (CSA)
- Interface to multi-vendor conditional access solutions

2. The Quest for Interoperability: Open Standards versus Licensing

Selection of open standards is a prerequisite for any modern digital television system. Adoption of open standards, however, is an insufficient criterion for ensuring interoperability. Digital television communications systems are extremely complex, dynamic and multi-faceted. Only by supplementing the use of open standards with a comprehensive licensing program will true interoperability of equipment from multiple suppliers be achieved. As networks continue to evolve, incorporating more innovations and improvements over time, the goal of interoperability will become increasingly dependent on cross-licensing and similar relationships between system developers and equipment suppliers.

Recognizing the fundamental distinction between adherence to open standards and achievement of interoperability, GI enhanced its commitment to standards compliance by commencing a broad-based licensing program. GI's "full systems" license encompasses all technological elements of GI's DigiCipher II digital television system. The user interface is independent of licensing, as it is primarily a consumer feature and an area for innovation and differentiation between consumer equipment from different suppliers. GI's extensive full disclosure allows licensees to develop and sell interoperable products for satellite, cable, MMDS, and other networks.

Licensees are not only provided with a full set of documentation, but they are also provided with engineering support to understand and implement the specifications properly. Importantly, GI's licensing framework includes improvements made to the system (by GI and/or its licensees) which relate to interoperability, so that all suppliers can remain interoperable over time. In addition, GI provides tools such as compliant bitstreams to its licensees and also performs